Prof. Dr. Stefan Wewers
Dipl.-Math. Julian Rüth
Institut für Reine Mathematik
Universität Ulm

WiMa-Praktikum II

Computeralgebra

SS 2014

Stand: 16.4.

In diesem Praktikum werden wir uns mit dem Lösen der sogenannten **Einheitengleichung** befassen. Sei R ein endlich erzeugter kommutativer Ring. Dann ist die Einheitengruppe $R^\times$ eine endlich erzeugte abelsche Gruppe. Wir betrachten die Gleichung

$$u + v = 1, \qquad u, v \in R^\times. \tag{1}$$

Ein berühmter Satz von Siegel besagt, dass diese Gleichung höchstens endlich viele Lösungen besitzt. Ziel des Praktikums ist, Algorithmen zu implementieren, die in interessanten Spezialfällen alle Lösungen der Einheitengleichung bestimmen.

Das wichtigste Hilfsmittel für das Lösen der Einheitengleichung sind sogenannte *Gitterreduktionsalgorithmen* wie zum Beispiel der LLL- oder der Fincke-Pohst-Algorithmus.

Wir werden systematisch das Computeralgebra-System SAGE verwenden. In einer Einführungsphase werden sich die Teilnehmer in dieses System einarbeiten, spezifische Kenntnisse von Sage sind aber nicht erforderlich. Alle Teilnehmer sollten mindestens die Vorlesung *Elemente der Algebra* gehört haben. Empfohlen sind weitere Kenntnisse in Algebra und Zahlentheorie, etwa durch die Master-Vorlesungen *Algebra* oder *Algebraische Zahlentheorie*.

1 Mathematische Grundlagen

1.1 Die S-Einheiten eines Zahlkörpers

Sei K ein *algebraischer Zahlkörper*, also eine endliche Körpererweiterung von $\mathbb{Q}$. Dann ist der Ganzheitsring $\mathcal{O}_K$ von K ein endlicher $\mathbb{Z}$-Modul und deshalb insbesondere ein endlich erzeuger Ring. Wir interessieren uns allgemeiner für

endlich erzeugte Teilringe $R \subset K$. Das wichtigste Beispiel hierfür sind die *S-Einheiten*.

Es sei $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ eine endliche Menge von Primidealen von $\mathcal{O}_K$. Eine Zahl $\alpha \in K$ heißt *S-ganz* falls

$$\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \quad \text{für alle } \mathfrak{p} \neq S.$$

Wir bezeichnen mit $\mathcal{O}_{K,S} \subset K$ die Teilmenge der S-ganzen Zahlen. Offenabr ist $\mathcal{O}_{K,S}$ ein Unterring von K, der $\mathcal{O}_K$ enthält.

Satz 1.1 *1. $\mathcal{O}_{K,S}$ ist ein endlich erzeugter Ring.*

2. Die Einheitengruppe $\mathcal{O}_{K,S}^{\times}$ von $\mathcal{O}_{K,S}$ ist endlich erzeugt und hat freien Rang $r + s$, wobei r der freie Rang von $\mathcal{O}_K^{\times}$ ist und $s := |S|$.

Bemerkung 1.2 Nach dem Dirichletschen Einheitensatz gilt $r = r_1 + r_2 - 1$, wobei (r_1, r_2) der Typ von K ist.

Beispiel 1.3 Es sei $K = \mathbb{Q}$. Dann gilt $\mathcal{O}_K = \mathbb{Z}$ und $S = \{p_1, \ldots, p_s\}$ ist eine endliche Menge von Primzahlen. Eine rationale Zahl $\alpha \in \mathbb{Q}$ is S-ganz, wenn sie von der Form

$$\alpha = a p_1^{x_1} \cdot \ldots \cdot p_s^{x_s}, \qquad \text{mit } a, x_i \in \mathbb{Z},$$

ist. Eine S-Einheit ist also von der Form

$$\epsilon = \pm \prod_i p_i^{x_i}, \qquad x_i \in \mathbb{Z}.$$

Die Gruppe der S-Einheiten wird erzeugt von -1 und den Elementen p_i von S.

1.2 Die Einheitengleichung

Es sei R ein endlich erzeugter Ring (es ist keine Einschränkung, $R = \mathcal{O}_{K,S}$ wie oben anzunehmen). Die *Einheitengleichung* ist die Gleichung

$$u + v = 1, \qquad u, v \in R^{\times}. \tag{2}$$

Satz 1.4 (Siegel, Mahler, Lang) *Die Gleichung* (2) *besitzt höchstens endlich viele Lösungen.*

Problem 1.5 Für $R = \mathcal{O}_{K,S}$ mit gegebenen K und S: bestimme sämtliche Lösungen von (2).

Der erste (und recht naive) Ansatz zur Lösung des Problems sieht so aus. Seien $u, v \in R^{\times}$ Einheiten. Diese haben eine eindeutige Darstellung

$$u = \zeta^a \prod_i p_i^{x_i}, \quad u = \zeta^b \prod_i p_i^{y_i},$$

mit $0 \leq a, b < n$ und $x_i, y_i \in \mathbb{Z}$. Sei $B > 0$ eine vorgegebene (große) Konstante. Dann können wir alle ganzen Zahlen a, b, x_i, y_i mit $0 \leq a, b < n$ und $|x_i|, |y_i| \leq B$ aufzählen und für jedes Tupel (a, b, x_i, y_i) die Identität $u + v = 1$ testen. Da die Gleichung (2) nach Satz ?? höchstens endlich viele Lösungen besitzt, erhalten wir auf diese Weise alle Lösungen von (2), wenn wir C hinreichend groß wählen. Eine Konstante C mit dieser Eigenschaft nennen wir eine *obere Schranke* für (2).

Diese Vorgehensweise (nennen wir sie die *Aufzählmethode*) hat zwei entscheidende Haken:

(a) Wenn wir keine obere Schranke C kennen, ist die Aufzählmethode keine echte Lösung des Problems. Wir können zwar prinzipiell alle Lösungen finden, wissen aber nicht, wielange wir warten müssen und wann wir fertig sind. Wir können also *niemals* sicher sein, dass wir alle Lösungen gefunden haben.

(b) Selbst wenn wir eine obere Schranke C kennen: ist C zu groß, so ist die Aufzählmethode praktisch nicht durchführbar, da wir eine Schleife über eine Menge mit $n^2 C^{2s}$ Elementen durchlaufen müssen.

Glücklicherweise kennt man obere Schranken, als Folge von einer bahnbrechenden Arbeit von Baker (??). Explizite obere Schranken für diverse Wahlen von K und S findet man z.B. in ???. leider sind die Schranken alle so groß, dass Sie die Aufzählmethode unpraktikabel machen. Siehe Beispiel ??.

Bemerkung 1.6 Sei

$$L := \{(u, v) \in (R^\times)^2 \mid u + v = 1\}$$

die Lösungmenge von (2). Dann definieren

$$(u, v) \mapsto (v, u), \qquad (u, v) \mapsto (u^{-1}, -u^{-1}v),$$

zwei Permutationen von L. (Insgesamt gibt es 6 solcher Permutationen.) Wir bezeichnen Lösungen aus L als *äquivalent* wenn Sie durch mehrfaches Anwenden obiger Permutationen ineinander überführt werden können. Da es ausreicht, alle Lösungen 'bis auf Äquivalenz' zu bestimmen, kann man diese Symmetrien häufig benutzen, um die Komplexität etwas zu reduzieren.

Ist zum Beispiel $K \subset \mathbb{R}$, so reicht es, Lösungen $(u, v) \in L$ mit

$$0 < u, v < 1$$

zu bestimmen, da jede Lösung zu einer solchen äquivalent ist.

Bemerkung 1.7 Sei $K = \mathbb{Q}$ und $S = \{p_1, \ldots, p_s\}$. Sei $(u, v) \in L$ eine Lösung mit $0 < u, v < 1$. Wir können dann $u = x/z, v = y/z$ mit $x, y, z \in \mathbb{N}$ paarweise teilerfremd schreiben. Es gilt dann

$$x + y = z,$$

wobei

$$x = \prod_i p_i^{x_i}, \;\; y = \prod_i p_i^{y_i}, \;\; z = \prod_i p_i^{z_i}, \quad x_i, y_i, z_i \geq 0.$$

Die paarweise Teilerfremdheit von x, y, z besagt, dass für jeden Index i höchstens eine der Zahlen x_i, y_i, z_i positiv ist. Wir setzen

$$m(x, y, z) := \max\{x_i, y_i, z_i \mid i = 1, \ldots, s\}.$$

Theorem 5.1 in [**?**] liefert eine explizite obere Schranke $C > 0$, sodass

$$m(x, y, z) \leq C$$

gilt für alle Lösungen $(u, v) \in L$.

Zum Beispiel für $S = \{2, 3, 5\}$ erhält man $C = 3.37 \times 10^{73}$. Es dürfte klar sein, dass diese Schranke für die Abzählmethode völlig unbrauchbar ist.

1.3 Gitterreduktion